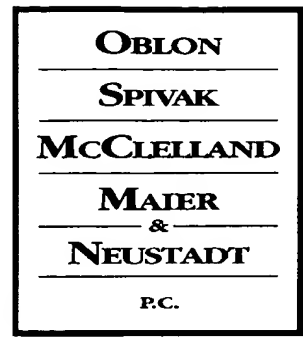


2157



Docket No.: 0039-7378-2RD



COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

ATTORNEYS AT LAW

ECKHARD H. KUESTERS  
(703) 413-3000  
EKUESTERS@OBLON.COM

KATHERINE D. PAULEY  
(703) 413-3000  
KPAULEY@OBLON.COM

RE: Application Serial No.: 09/404,547  
Applicants: Takeshi SAITO, et al.  
RCE Filed: December 8, 2003  
For: RELAY DEVICE AND COMMUNICATION DEVICE  
REALIZING CONTENTS PROTECTION  
PROCEDURE OVER NETWORKS  
Group Art Unit: 2157  
Examiner: TODD, G.

RECEIVED

FEB 18 2004

Technology Center 2100

SIR:

Attached hereto for filing are the following papers:

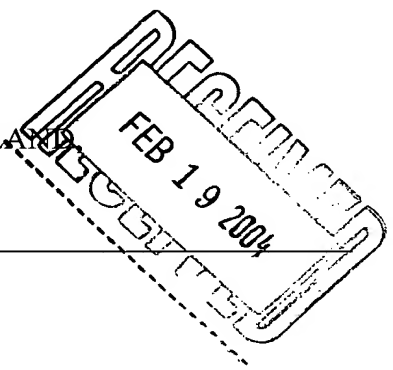
- Filing of Statement of Relevancy
- Statement of Relevancy
- Copy of 12/8/03 Filing Receipt
- Copy of IDS Transmittal Filed 12/8/03
- Copy of PTO 1449 Form Filed 12/8/03
- Copy of Japanese Article Listed at AY on 1449 Filed 12/8/03

Our check in the amount of \$0.00 is attached covering any required fees. In the event any variance exists between the amount enclosed and the Patent Office charges for filing the above-noted documents, including any fees required under 37 C.F.R. 1.136 for any necessary Extension of Time to make the filing of the attached documents timely, please charge or credit the difference to our Deposit Account No. 15-0030. Further, if these papers are not considered timely filed, then a petition is hereby made under 37 C.F.R. 1.136 for the necessary extension of time. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND  
MAIER & NEUSTADT, P.C.

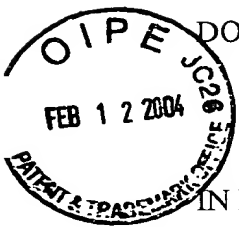
*Katherine D. Pauley*  
Eckhard H. Kuesters  
Registration No. 28,870



Customer Number  
**22850**

(703) 413-3000 (phone)  
(703) 413-2220 (fax)  
I:\ATTY\KDP\0039\0039 7378\0039 7378 PTO CVR LTR.DOC

Katherine D. Pauley  
Registration No. 50,607



DOCKET NO: 0039-7378-2RD

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF :

TAKESHI SAITO, ET AL. :

EXAMINER: TODD, G.

SERIAL NO: 09/404,547 :

RCE FILED: DECEMBER 8, 2003 :

GROUP ART UNIT: 2157

FOR: RELAY DEVICE AND  
COMMUNICATION DEVICE REALIZING  
CONTENTS PROTECTION PROCEDURE  
OVER NETWORKS

FILING OF STATEMENT OF RELEVANCY

**RECEIVED**

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

FEB 18 2004

Technology Center 2100

SIR:

Applicants wish to provide the enclosed Statement of Relevancy, corresponding to the Japanese article previously filed December 8, 2003, listed at line AY on the PTO 1449 Form. A copy of the date-stamped filing receipt, IDS Transmittal, PTO 1449 Form, and Japanese article listed at line AY, is enclosed herewith.

Please charge any fees for the papers being filed herewith for which no check or credit card payment is enclosed herewith to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters  
Registration No: 28,870  
Attorney of Record  
Katherine D. Pauley  
Registration No: 50,607

**Customer Number**  
**22850**

Tel No (703) 413-3000  
Fax No (703) 413-2220  
EHK:KDP:dmr

I:\ATTY\KDP\0039\0039 7378\0039 7378 FILING STAT OF REV.DOC

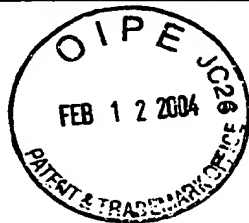
DOCKET NO.: 0039-7378-2RD

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

IN RE APPLICATION OF:

Takeshi SAITO, et al.

SERIAL NO: 09/404,547



GROUP: 2157

RCE FILED: December 8, 2003

EXAMINER: TODD, G.

FOR: RELAY DEVICE AND COMMUNICATION DEVICE REALIZING  
CONTENTS PROTECTION PROCEDURE OVER NETWORKS

**RECEIVED**

FEB 18 2004

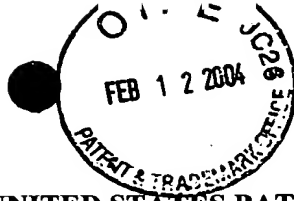
**STATEMENT OF RELEVANCY**

Technology Center 2100

This reference discloses the fact that receiving an encryption key information at a relay node and transmitting that information simply to a destination is well known in the encryption scheme in general. For example, this reference discloses that, in the key exchange according to the ISAKMP negotiation, the negotiation is carried out by forming a tunnel between the transmitting side and the receiving side, and this disclosure can be construed as implying that the relay device that constitutes the tunnel will simply transfer the key information to a destination.

However, this reference by itself does not suggest or imply the relay device or the communication device as recited in the claims of the present application.

Docket No. 0039-7378-2RD



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF: Takeshi SAITO et al.

SERIAL NO: 09/404,547

GAU: 2157

RCE FILED: HEREWITH

EXAMINER: TODD, G.

FOR: RELAY DEVICE AND COMMUNICATION DEVICE REALIZING CONTENTS PROTECTION PROCEDURE  
OVER NETWORKS

INFORMATION DISCLOSURE STATEMENT UNDER 37 CFR 1.97

COMMISSIONER FOR PATENTS  
ALEXANDRIA, VIRGINIA 22313

RECEIVED

FEB 18 2004

Technology Center 2100

SIR:

Applicant(s) wish to disclose the following information.

REFERENCES

- ☒ The applicant(s) wish to make of record the references listed on the attached form PTO-1449. Copies of the listed references are attached, where required, as are either statements of relevancy or any readily available English translations of pertinent portions of any non-English language references.
- ☐ A check or credit card payment form is attached in the amount required under 37 CFR §1.17(p).

RELATED CASES

- ☐ Attached is a list of applicant's pending application(s) or issued patent(s) which may be related to the present application. A copy of the patent(s), together with a copy of the claims and drawings of the pending application(s) is attached along with PTO 1449.
- ☐ A check or credit card payment form is attached in the amount required under 37 CFR §1.17(p).

CERTIFICATION

- ☐ Each item of information contained in this information disclosure statement was first cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of this statement.
- ☐ No item of information contained in this information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application or, to the knowledge of the undersigned, having made reasonable inquiry, was known to any individual designated in 37 CFR §1.56(c) more than three months prior to the filing of this statement.

DEPOSIT ACCOUNT

- ☒ Please charge any additional fees for the papers being filed herewith and for which no check or credit card payment is enclosed herewith, or credit any overpayment to deposit account number 15-0030. A duplicate copy of this sheet is enclosed.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,  
MAIER & NEUSTADT, P.C.

Eckhard H. Kuesters

Registration No. 28,870

David A. Bilodeau

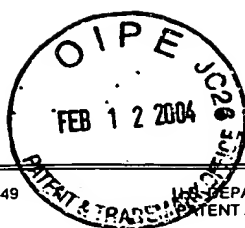
Registration No. 42,325

Customer Number

22850

Tel. (703) 413-3000  
Fax. (703) 413-2220  
(OSMMN 05/03)

COPY



Form PTO 1449 (Modified)		U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE		ATTY DOCKET NO. 0039-7378-2RD		SERIAL NO. 09/404,547	
LIST OF REFERENCES CITED BY APPLICANT				APPLICANT Takeshi SAITO et al.			
				FILING DATE RCE FILED HEREWITH		GROUP 2157	
				U.S. PATENT DOCUMENTS			
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUB CLASS	FILING DATE IF APPROPRIATE
	AA						
	AB						
	AC						
	AD						
	AE						
	AF						
	AG						
	AH						
	AI						
	AJ						
	AK						
	AL						
	AM						
	AN						
FOREIGN PATENT DOCUMENTS							
		DOCUMENT NUMBER	DATE	COUNTRY	TRANSLATION YES NO		
	AO	10-145420	05/29/98	JAPAN W/ENGLISH ABSTRACT			XX
	AP	10-154996	06/09/98	JAPAN W/ENGLISH ABSTRACT			XX
	AQ						
	AR						
	AS						
	AT						
	AU						
	AV						
OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, etc.)							
	AW	Takashi Sato, Philips Research Briarcliff, "A SOLUTION TO WIRELESS CONNECTIONS IN MULTI-BUS NETWORK," June 9, 1998, pgs. 1-8					
	AX	"5C Digital Transmission Content Protection White Paper," Hitachi, Ltd., Intel Coporation, Matsushita Electric Industrial, Co., Ltd., Sony Corporation and Toshiba Corporation, July 14, 1998, 15 pgs.					
	AY	N. Yokokawa, "Understanding IPsec which is Indispensable to Security System Standard," Computer and Network Lan, Vol. 16, No. 7, July 1998, 6 pgs.					
	AZ					<input type="checkbox"/> Additional References sheet(s) attached	
Examiner					Date Considered		
*Examiner: Initial if reference is considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.							

COPY

**特集**

TCOを考えたセキュリティ戦略

## セキュリティ・システムの標準に 不可欠のIPSecを理解する

日本シスシステムズ(株)  
マーケティング本部

横川 典子

- インターネットがビジネスのインフラストラクチャとなったいま、不正行為を防止する技術が不可欠となってきた。IPSecは、セキュリティに弱いといわれていたIPに、セキュリティ機能をもたせるためにIETFで標準化が進められている新しいプロトコルだ。次世代IPであるIPv6のためのセキュリティ技術として開発されはじめたが、現行のIPv4でも利用が可能になっている。

### ネットワーク層の暗号化を 提供するIPSec

IPSecの提供するセキュリティは、認証と暗号化から構成される。

暗号化はセキュリティ技術の代表的なものだ。通信を安全にするために、暗号化メールなど、アプリケーションごとに暗号化を行うという方法もある。これに対し、IPSecはIPの、つまりネットワーク層における暗号化を提供している。ネットワーク層で暗号化を行うことにより、個々のアプリケーションは必ずしも暗号化対応でなくても、安全な通信が行えるようになる。ネットワーク層にIPSecを導入すれば、それぞれ暗号化対応のアプリケーションを用意する必要はないということである。IPSecはアプリケーションに対して透過的にセキュリティを提供しているといえる。このとき、データリンクなど、下位の層も変更の必要はない。

### IPSecを変える セキュリティ技術とは

IPSecは異なるいくつかのセキュリティ技術を組み合わせることによって、完全なセキュリティ・システムとして動作する。

- Diffie-Hellman 鍵交換アルゴリズム

盗聴される可能性のあるインターネット上で、秘密通信を行おうとしている二者が共通する秘密（共通鍵）を作成/交換するためのアルゴリズム。

- 公開鍵暗号

Diffie-Hellman 鍵交換で、第三者による盗聴などの攻撃を防止しながら、二者間で互いの身元を保証するために用いられる認証システムとしての公開鍵暗号の利用。

- 高速な暗号化アルゴリズム

メッセージ全体を暗号するのに用いる、大量のデータを高速に処理できるDESなどの暗号化アルゴリズム。

- キード・ハッシュ (keyed hash) によるアルゴリズム

MD5やSHAなどのハッシュ関数と組み合わせて用いるHMACなどのkeyed Hashアルゴリズム。

- 電子承認 (Digital Certificate)

電子IDカードのような役割を果たす、CA (Certificate Authority) による承認 (Certificate)

IPSec は以上のようなセキュリティ技術を組み合わせてネットワーク・セキュリティを提供するためのシステムである。詳細は、RFC1826-1829や、いくつかの Internet Drafts として提供されている。

## セキュリティ・アソシエーション (Security Association/SA)

IPSec では、セキュリティ・アソシエーション (SA) という言葉がよく使われる。IPSec による通信を行うときには、どのくらいのレベルのセキュリティ・サービスが提供されるのか (完全性 (途中で改ざんされていないこと)、安全性など) を、通信しようとする二者 (それ以上の場合もあるがここでは二者とする) 間で決定しなければならない。サービスが決定すると、次に暗号化を行う場合にはどのアルゴリズムを使うかを決めて、さらに秘密鍵の生成/交換を行わなければならない。これらの複雑な手続きを終えた結果結ばれた二者の関係をセキュリティ・アソシエーションと呼ぶ。SA は、AH や ESP という IPSec 独自のヘッダに含まれる、SPI (Security Parameters Index) と呼ばれる一意の乱数と送信先の IP アドレスを元に識別される。SA とは、二者間で取り交わされた、セキュリティ・ポリシーであるということができる。

SA の確立方法については、後述する ISAKMP/Oakley の項で説明する。

## IPSecのヘッダ

IPSec では、通常の IP ヘッダに加え、新たに2つのヘッダを用いている。これらのヘッダは、IP ヘッダとトランスポート層ヘッダ (TCP ヘッダまたは UDP ヘッダ) との間に挿入されて使われる。

### ● Authentication Header (AH)

AH は、IP パケットの完全性と、パケットの送信

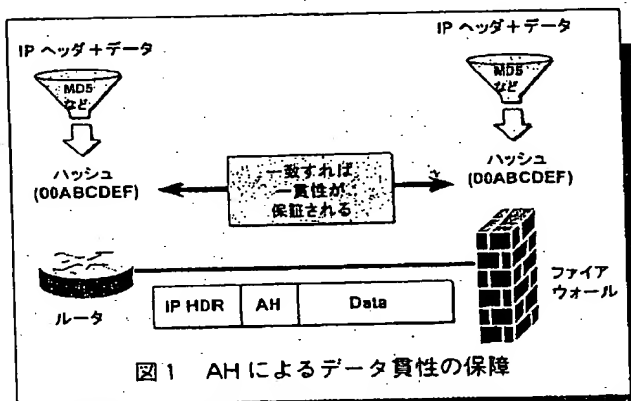


図1 AHによるデータ真性の保障

元の認証機能を果たすが、暗号化機能は提供していない。AH はキード・ハッシュを用いて、完全性および認証機能を提供している。AH は SA を識別するための SPI とハッシュの結果を格納する Authentication Data などから構成される。

発信元 A は、IP パケット全体を MD5 などのハッシュ関数にかけ、その結果を AH 中の Authentication Data に入れて送信先 B へ送る。

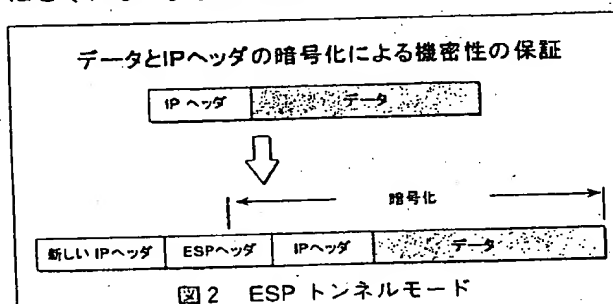
B は受けとった IP パケットから AH をとり除き、そこから Authentication Data をとり出す。そして AH をとり除いた IP パケットを同じハッシュ関数にかけてハッシュを得て、その結果を Authentication Data にあったハッシュと比較する。もし2つのハッシュが等しければ、その IP パケットは、ヘッダを含め改ざんされていないことが証明される。「ヘッダを含め改ざんされていない」ということはつまり、発信元アドレス・フィールドの値も変更されていないということになり、結果として発信元の認証機能を果たしている (図1)。

## Encapsulating Security Payload (ESP)

ESP は、IP パケットを暗号化することにより、機密性を提供するものである。ESP は SA を識別するための SPI と、暗号化されたデータである Transform Data などから構成される。

ESPには、暗号化の対象となる範囲が違う2つのモード、トランスポート・モードとトンネル・モードがある。トランスポート・モードはオリジナルのIPパケットのペイロード部（IPヘッダ以降の部分）が暗号化され、IPヘッダは暗号化されず、そのまま送信パケットのヘッダとして利用される。トンネル・モードでは、オリジナルのIPパケットのヘッダごと暗号化され、新たにIPヘッダを付け直す（図2）。

AHとESPは単独で用いることもできるし、同時に組み合わせて用いることもできる。キードハッシュ・アルゴリズムや暗号アルゴリズムに関する規定はとくにない。安全な通信を行おうとする二者間で

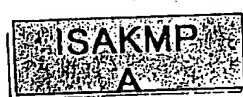


合意があれば、どのアルゴリズムを使ってもかまわない。しかし、任意の相手との通信を保証するため、最低限サポートしなければならないアルゴリズムが規定されている。RFC1828では、ハッシュ・アルゴリズムとしてKeyed MD5を、RFC1829では暗号化アルゴリズムとしてDES (CBC) をサポートすることとしている。

## ISAKMP/Oakley

以上で述べたIPSec通信は、二者がすでに、SAの関係にあることを前提としている。ISAKMP/OakleyはSAの確立のためのネゴシエーションを行う。まずSAを結ぶ前に、互いに認証をしあわなければならない（図3）。ISAKMP/Oakleyは二者、たとえばAとBとの間にトンネルを張り、互いを認証し、セキュリティ・サービスに関するネゴシエーションを行う。ネゴシエーションが終了した時点で、AとBとはSA関係にあることになり、IPSecによる通信

### ① まだ、SAは確立していない



### ② AのISAKMPがBのISAKMPとネゴシエーション

### ④ AとBはIPSecを使って通信を行う



### ③ ネゴシエーションが終了し、AとBはSAの関係になる

図3 ISAKMPを使ったSAの確率



特集

TCOを考えた  
セキュリティ戦略

が可能な状態となる。IPSecで利用される秘密鍵はISAKMP/Oakleyの秘密鍵とは異なるが、ISAKMP/Oakleyのトンネルを張る際にDiffie-Hellmanを使って作成した鍵をリフレッシュして用いるか、もう一度Diffie-Hellmanを使って鍵を生成し直す。どちらの方法をいつ用いるかに関しても、SAを生成する際に交渉される。

## IPSecの応用

IPSecは、いってみればVPNのセキュリティ機能用の標準プロトコルである。まだまだコストのかかる専用線の契約をしなくても、IPSecを使えば任意のサイトと安全通信を行うことができるようになる。とくにE-Commerceやエクストラネットなどのネットワーク上の商用取り引きが盛んになる今後、単に支社、支店といった関連組織だけではなく、取引先や客、パートナーなどの組織とも安全通信を行う必要が出てくる。このとき、コストのかかる専用線を引かなくても、IPSecを利用すれば、バーチャルな専用線ネットワーク（Virtual Private Network）を利用して安全な通信が行えるようになるのだ。

実際にVPN用プロトコルとして用いられるほかに、IPSecはVPDN（Virtual Private Dial Network）サービスにおけるセキュリティ技術としての利用の可能性もある。VPDNはデータリンク層フレームをIPパケットでカプセル化し、インターネット上でトンネリング通信を提供する技術だが、暗号化がオプションになっている。IPSecという標準化された暗号化技術があれば、暗号化に関してはネットワーク層

のIPSecの機能を借りて提供することができるようになる。

## 相互接続性とCiscoのIPSecへの取り組み

IPSecの目的は、インターネット上の安全な通信であるが、もう一つの、相互接続性の提供という大きな目標ももつ。

多くの暗号化アプリケーションは、暗号化対応アプリケーション同士でないと安全な通信が行えない、という問題を抱えており、IPSecはネットワーク層でこの問題を解決しようとしているのである。

ANX（Automotive Network eXchange）は、IPSecの相互接続性を促進させる動きとして注目されている。GM、フォードら米国自動車メカなどが互いに安全な通信を行う目的で結成されたこの組織は、ベースとなる技術としてIPSecを採用し、相互接続実験を開始している。

CiscoSystemsもCiscoIOSを提供した。CiscoSystemsは従来から提供してきたPIX Private LinkやCiscoIOSドライバなどを提供していく予定である。また、IETFにおいても、ISAKMP/Oakleyを提案するなど、IPSecの標準化にも貢献している。

IPSecはIETFによって標準化が進められている公開された仕様であり、任意のエンドポイント間の安全な通信を保証する。IPがそうであったように、仕様に従うかぎり実装は自由である。このオープン・アーキテクチャのもつ性質がIPSecの普及を促進させ、結果としてインターネットの安全性の向上に貢献していくことであろう。

## 絵ときフレーム・リレー活用バイブル—NTTのフレーム・リレー・サービス—

NTTフレームリレー研究会 編

B5判 144頁 定価（本体2900円【税別】）

（※本体価格の変更、品切れが生ずる場合があります。）

Ohmsha

# コンピュータネットワークLAN

## 特集 TCOを考えたセキュリティ戦略

特別レポート 3層スイッチングHUBとギガビット・  
スイッチングHUBの評価テスト

ネットワーク①超高速通信向けリンク・レイヤ・プロトコル「MAPOS」  
ネットワーク②ギガビットEthernet「BL-3000」による超高速ネットワーク構築法  
デバイス「NEC NX7000」で全社グループウェアを構築した住友生命



オーム社ホームページ

<http://www.ohmsha.co.jp/>

私に、特別な知識など要らない。

導入から運用・セキュリティまで、インターネット環境をトータルサポート。

net  
**GUARDIAN**  
ALL IN ONE PACKAGE

New BL-3000

New BL-3000は、NTTが世界各国のメーカー・ベンダーとの協力のもとに提供する情報通信システム構築製品です。

NTT



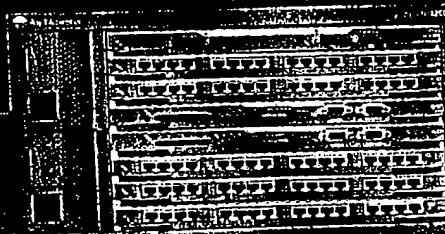
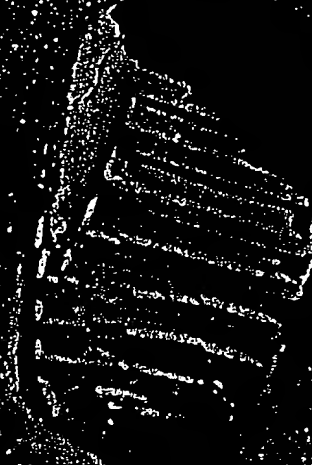
Bay Networks Where Information Flows.

インターネット・LAN

●発行 昭和55年5月 ●昭和55年5月11日 第3回郵便物認可 ●1996年7月1日発行 (毎月1回) ●株式会社オーエム社 第16巻7号・通巻177号

# 先駆者。

一九六九年アメリカは他国に先駆けて月面着陸に成功し、宇宙という新しい世界を開く。  
一九九七年、ギガビット・ルーティング・スイッチの登場により、  
ビジネス通信の新しい世界の扉が開けます。



## Accelar<sup>TM</sup> 1200

ギガビット・ルーティング・スイッチ

● ASICが実現した157bps スイッチ・ファブリック ● 最大1G×12ポート収容可能 ● 第三者機関による評価で700万パケット超という驚異的な性能

ベイ・ネットワークス株式会社

〒05-6026 東京都港区赤坂/194-3-1 Bay Networksのロゴ、AccelarはBay Networks Inc.の登録商標です。  
その他の登録された社名及び製品名等は、各社の商標または登録商標です。

<http://www.baynetworks.co.jp>

販売代理店 東京 青木通信株式会社

TEL.03-5412-8639

